CLAIMS

1. An apparatus for generating pseudorandom sequences characterized by comprising:

cellular automata of a first type for generating a first sequence with higher randomness;

cellular automata of a second type for generating a second sequence with predetermined lower bound on the period; and

adders for performing bit-to-bit mod2 sum of the first sequences and the second sequences.

2. The apparatus according to claim 1, characterized in that:

the cellular automata of a first type is two-dimensional cellular automata;

the cellular automata of a second type is 2-by-L cellular automata; and

the summation results from the adders are outputted as the pseudorandom sequences.

3. The apparatus according to claim 1, characterized by further comprising:

cellular automata of a third type for generating a third sequence, the cellular automata of a third type having cells whose states can be computed based on corresponding cell control word and/or rule control word; wherein

the cell control word is generated by the cellular automata of a second type;

the rule control word is generated by the cellular automata of a first type; and

the adders for performing bit-to-bit mod2 sum of the first, the second and the third sequences.

4. The apparatus according to claim 3, characterized in that:

the summation results from the adders are outputted as the pseudorandom sequences.

5. The apparatus according to claim 2 or claim 4, characterized by further comprising:

a block for performing nonlinear mapping on the summation results from the adders; and

a block for perform non-uniform decimation on the results of the nonlinear mapping;

wherein the decimated result is outputted as the pseudorandom sequence.

6. The apparatus according to claim 5, characterized in that:

each of the blocks includes at least one nonlinear function.

7. The apparatus according to claim 5, characterized in that:

the block for performing nonlinear mapping includes at least one look-up table for nonlinear mapping based on the Latin squares.

8. An apparatus for performing cryptographic processing characterized by comprising:

a cryptographic processor for encrypting data using pseudorandom sequences; and

a pseudorandom sequence generator for generating the pseudorandom sequences;

wherein the pseudorandom number generator is configured to include the apparatus according to any one of claims 1-7.

9. A method for generating pseudorandom sequences using cellular automata characterized by comprising the steps of:

generating a first sequence with higher randomness;

generating a second sequence with predetermined lower bound on the period; and

performing bit-to-bit mod2 sum of the first sequences and the second sequences.

10. A computer program for causing a computer to execute a method for generating pseudorandom sequences using cellular automata, the computer program characterized in that:

the method includes the steps of

generating a first sequence with higher randomness;

generating a second sequence with predetermined lower bound on the period; and

performing bit-to-bit mod2 sum of the first sequences and the second sequences.

11. A recording medium storing a computer program for causing a computer to execute a method for generating pseudorandom sequences

using cellular automata, the recording medium characterized in that:

the method includes the steps of

generating a first sequence with higher randomness;

generating a second sequence with predetermined lower bound on the period; and

performing bit-to-bit mod2 sum of the first sequences and the second sequences.